DETAILED ACTION

1> This action is in response to Applicant's request for continued examination. Claims 1 and 9 are amended. Claims 1-16 are presented for further examination.

2> This action is a non-final rejection.

Continued Examination Under 37 CFR 1.114

3> A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 5.9.2008 has been entered.

Response to Arguments

4> Applicant's arguments with respect to claims 1-16 have been considered but are moot in view of the new ground(s) of rejection necessitated by Applicant's amendment. Applicant raises two issues against Rabne and the motivation for combining references with Rabne. Since Rabne is still utilized as the primary reference in the new ground of rejection, Applicant's arguments are addressed here.

First, Applicant argues that Rabne does not teach or mention a proxy system. Examiner first notes that Applicant's Figure 1 is an exemplary drawing of Applicant's invention. The figure displays various elements of Applicant's invention including an end user, an Aereous server, and

network storage. Just like Rabne, Figure 1 does not even mention a proxy system. Clearly, one of ordinary skill in the art would have interpreted Applicant's Aereous server as the proxy between the end user and the network storage because the Aereous server acts in place of the end user to communicate with the network storage. Indeed, Applicant's specification refers to the Aereous server as a proxy system [Figure 1 «item 110» | pg. 16, line 10].

Thus, while not expressly disclosing the exact term "proxy system," Rabne still discloses a proxy system as claimed by Applicant. Specifically, Rabne discloses a rights management server that, like Applicant's claimed proxy system, is situated between an end user and network storage [Figure 1b «items 10, 20, 22»]. Because the rights management server receives and responds to requests from the end user in place of the network storage [column 7 «lines 5-9»], one of ordinary skill in the art would have interpreted Rabne's rights management server as a proxy system for the end user client.

Second, Applicant argues, without discussion or support, that the previous rejection relied on Applicant's disclosure as hindsight to assemble teachings from disparate references to arrive at Applicant's claimed invention. However, beyond a generalized accusation that the references are disparate, Applicant supplies no support for arguing the rejection relied on hindsight.

Rabne is directed towards a security system for controlling access to digitized data. Rabne accomplishes this through the use of rights and permissions that control the type of access to data that a user is permitted. Similarly, the newly cited reference, O'Brien is directed towards a security system for also controlling access to data in a computer system. And Taylor also discloses a security system that protects files on a computer system.

Therefore, Applicant's arguments as the rejection's reliance on hindsight reconstruction are not persuasive. Additionally, this action contains a new ground of rejection which render Applicant's arguments as to the Rabne, Chan, and Taylor combination moot. If Applicant maintains this argument in future correspondences, Applicant should supply reasons as to why one of ordinary skill in the art would not have combined the references as suggested by the Office action.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5> Claims 1-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rabne et al. (U.S. Patent Number 6,006,332), hereinafter referred to as Rabne, in view of O'Brien et al, U.S. Patent No. 6.658.571 ["O'Brien"], further in view of Taylor et al, U.S Patent No. 6.728.885 ["Taylor"].

6> Rabne disclosed a system for controlling access to and protecting use of digitized data utilizing a secure rights management server. In an analogous art, O'Brien is directed towards a security framework utilizing kernel-based security modules to protect file systems by controlling access to and protecting use of computer files. Also in an analogous art, Taylor disclosed a

security system for filtering packets by utilizing, in part, a module operating at the kernel level to examine packets to protect computer systems.

7> Concerning claims 1 and 9, Rabne did not explicitly state a client module configured to interface to a client operating system kernel and configured to enforce a set of usage rights within the operating system kernel without application rewrites, wherein enforcing the set of usage rights includes: intercepting a system call between an application and the client OS, evaluating the system call based on the set of usage rights, and blocking or modifying the system call based on said evaluation. However, allowing a system to enforce access rights in an operating system kernel by intercepting system calls and evaluating the system call based on the access rights was a well known feature in the art as evidenced by O'Brien whose system uses a security mechanism at the operating system level to determine usage rights for users or processes. Further, as discussed above, the limitation "without application rewrites" is merely an effect of performing the enforcement within the OS kernel. Thus, since O'Brien discloses enforcing usage rights at the OS level, O'Brien implicitly teaches the limitation.

It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to modify the system of Rabne by adding the ability to use a client module configured to interface to a client operating system kernel and configured to enforce a set of usage rights within the operating system kernel by intercepting system calls and evaluating the system calls based on the set of usage rights as provided by O'Brien. Here the combination satisfies the need for a system to control and monitor the access and use of restricted content on a network. See

Rabne, column 3, lines 32-38. Additionally, O'Brien's kernel level enforcement provide more protection than traditional security routines [see O'Brien, column 3 «lines 61-64»].

8> Also concerning claims 1 and 9, the combination of Rabne and O'Brien did not explicitly state obtaining the content on an individual block basis. Rabne, who teaches the distribution of intellectual property over a network, is not specific on how this content is transferred; for example Rabne is not specific as to whether it is transferred on an individual block basis. However, obtaining content comprising data blocks from content sources on an individual block basis is well known in the art as evidenced by Taylor whose system receives and filters each data packet (which are transmitted individually) as well as a set of access policies that comprise a set of predefined usage policies associated with the content for said user. Taylor's packets correspond to Applicant's claimed "block."

It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to modify the combination of Rabne and O'Brien by adding the ability to obtain content on an individual block basis as well as the access policies that comprise predefined usage policies associated with the content for the user as provided by Taylor. Here the combination satisfies the need for a system to control and monitor the access and use of restricted content on a network. See Rabne, column 3, lines 32-38. The combination also improves Rabne's system as it provides users the capability of dynamically filtering individual packets [Taylor, column 4 «lines 8-12»].

9> Some claims will be discussed together. Those claims which are essentially the same except that they set forth the claimed invention as a method are rejected under the same rationale applied to the described claim.

10> Thereby, the combination of Rabne, O'Brien, and Taylor discloses:

- <Claims 1 and 9>

A dynamic file access control and management system configured to access one or more content sources including a set of content, said system comprising:

A. a proxy system linked to said one or more content sources, said proxy system comprising an access control module configured to selectively obtain content comprising data blocks from said content sources on an individual block basis as a function of an authorization of a user requesting said content and a set of access policies (Rabne, column 7, lines 5-9 and column 8, lines 55-67, where Taylor teaches obtaining the data on an individual block basis, column 1 «lines 63-65» | column 5 «lines 32-39») that comprise a set of predefined usage policies associated with the content for said user (Rabne, column 8, lines 11-14 and 34-37 – Rabne's license agreement reads on Applicant's claimed usage policy);

B. a rights management module configured to generate a set of usage rights associated with said content as a function of a set of predefined usage policies associated with said content for said user (Rabne, column 8, lines 11-37 – permissions rights generated from the license agreement);

C. at least one client device having a client module configured to interface to a client operating system kernel, said client module configured to enforce the set of usage rights within the operating system kernel without application rewrites (Rabne, column 6, lines 31-45 and O'Brien, column 3 «lines 39-55» : O'Brien's kernel-level security modules apply security policies by granting or denying access to resources), wherein enforcing the set of usage rights includes:

intercepting a system call between an application and the client OS [O'Brien, column 5 «lines 28-36» | column 7 «lines 10-12»];

evaluating the system call based on the set of usage rights [O'Brien, column 5 «lines 56-66» | column 7 «lines 27-40»]; and

blocking or modifying the system call based on said evaluation [O'Brien column 5 «line 67» to column 6 «line 4» | column 7 «lines 41-48»];

D. one or more communication means, via which said content and said usage rights are provided to said client device (Rabne, column 3, lines 52-59).

- <Claims 2 and 10>

The system according to claim 1, wherein said content and said usage rights are provided to said client device via different communication means (Rabne, column 10, lines 34-48).

- <Claims 3 and 11>

The system according to claim 1, wherein said content includes static content (Rabne, column 6, lines 53-60).

- <Claims 4 and 12>

The system according to claim 1, wherein said content includes dynamic content (Rabne, column 6, lines 53-60).

- <Claims 5 and 13>

  The system according to claim 1, wherein said communication means includes a secure transform configured to encrypt and encapsulate said content into a message as a function of a session ID and said client is configured to extract said content from said message (Rabne, column 7, lines 10-19).

- <Claims 6 and 14>

  The system according to claim 1, wherein said proxy system further includes a user interface, configured to facilitate creation and editing of said access policies and said usage policies and association of said access policies and said usage policies with said content (Rabne, column 18, lines 20-32 and 50-67).

- <Claims 7 and 15>

  The system as in claim 1, wherein said client device is a device from a group comprising: 1) a personal computer; 2) a workstation; 3) a personal digital assistant; 4) an e-mail device; 5) a cellular telephone; 6) a Web enabled appliance; and 7) a server (Rabne, column 6, lines 31-45).

- <Claims 8 and 16>

  The system of claim 1, wherein said proxy system and at least one of said content sources are hosted on the same computing device (Rabne, figure 1b, item 22).

Since the combination of Rabne, O'Brien, and Taylor discloses all of the above limitations, claims 1-16 are rejected.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DOHM CHANKONG whose telephone number is (571)272-3942. The examiner can normally be reached on Monday-Friday [8:30 AM to 4:30 PM].

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Bunjob Jaroenchonwanit can be reached on 571.272.3913. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Dohm Chankong/
Examiner, Art Unit 2152